WHAT IS CLAIMED IS:

1. A method for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising the steps of:

transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer;

transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter;

transmitting a blank electronic ballot, upon request by the registered voter at a second computer, from the computer database that resides on the transaction repository server, via the transaction mediator, to the second computer; and

transmitting a voted electronic ballot from the second computer, via the transaction mediator, to the computer database that resides on the transaction repository server.

2. The method of claim 1, comprising:

establishing at least one computer database on the transaction repository server that contains information associated with at least one of a voter registration status of a citizen and a electronic ballot status;

requesting a status at the first computer from the transaction repository server;

determining a status message in response to the step of requesting by examining the at least one computer database; and

transmitting the status message from the transaction repository server to the first computer.

3. The method of claim 2, wherein the voter registration status of the citizen and the electronic ballot status are verified.

4. The method of claim 1, wherein the network includes:

an encrypted communication channel between at least one of the first and second computer and the transaction mediator, and an encrypted communication channel between the transaction mediator and the transaction repository server.

5. The method of claim 1, wherein the registration information includes at least one descriptive element associated with a citizen.

6. The method of claim 1, wherein the step of transmitting registration information comprises:

entering the registration information; and

digitally signing the registration information using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of a citizen, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the registration information.

7. The method of claim 6, wherein the step of transmitting registration information comprises:

erasing from the first computer information associated with the registration information once the registration information has been transmitted.

8. The method of claim 6, wherein the step of transmitting registration information comprises:

verifying the digital signature using the public key of the public-private key pair.

9. The method of claim 6, wherein the public-private key pair and the cryptographic identification can be used by the citizen with respect to a plurality of electronic transactions.

10. The method of claim 1, wherein the step of transmitting registration information comprises:

approving or denying a voting registration request at the computer database based on the registration information of a citizen.

11. The method of claim 1, wherein the second computer is the first computer.

12. The method of claim 1, wherein the step of transmitting a blank electronic ballot comprises:

digitally signing the blank electronic ballot using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of an operator of the transaction repository server, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the blank electronic ballot; and

transmitting a public key of a public-private key pair of the transaction repository server.

13. The method of claim 1, wherein the step of transmitting the voted electronic ballot comprises:

executing the blank electronic ballot;

encrypting the voted electronic ballot using a symmetric cryptographic function and a symmetric key that is randomly generated by the second computer;

encrypting the symmetric key using a public key of a public-private key pair of the transaction repository server; and

digitally signing the encrypted voted electronic ballot and the encrypted symmetric key using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of the registered voter, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the voted electronic ballot.

14. The method of claim 13, comprising:

erasing from the second computer information associated with the encrypted voted electronic ballot once the voted electronic ballot has been transmitted.

15. The method of claim 13, comprising:

verifying the digital signature of the encrypted voted electronic ballot and the encrypted symmetric key using the public key of the public-private key pair of the registered voter.

16. The method of claim 13, comprising:

reconciling transmitted voted electronic ballots by an operator of the transaction repository server to establish the validity of each transmitted voted electronic ballot.

17. The method of claim 16, comprising:

separating a plurality of valid encrypted voted electronic ballots into groups based on at least one characteristic;

stripping the digital signature and the cryptographic identification of the registered voter from each group of valid encrypted voted electronic ballots; and

randomly mixing within each group the separated encrypted voted electronic ballots.

18. The method of claim 17, wherein the at least one characteristic is a type of voted electronic ballot.

19. The method of claim 17, comprising:

decrypting the encrypted symmetric key of each separated voted electronic ballot using a private key of the public-private key pair of the transaction repository server;

decrypting the encrypted voted electronic ballot using the symmetric key to recover the voted electronic ballot; and

printing the voted electronic ballot.

20. A method for verifying at least one of a voter registration status and an electronic ballot status in a voting system, comprising the steps of:

establishing at least one computer database on a transaction repository server that contains information associated with at least one of the voter registration status of a citizen and the electronic ballot status;

requesting a status at a first computer from the transaction repository server;

determining a status message in response to the step of requesting by examining the at least one computer database; and

transmitting the status message from the transaction repository server to the first computer.

21. The method of claim 20, wherein a transaction mediator communicates information between the first computer and the transaction repository server.

22. The method of claim 20, wherein the voter registration status of the citizen and the electronic ballot status are verified.

23. A method for completing and submitting an electronic voter registration form and an electronic ballot transmitted over a network, comprising the steps of:

transmitting registration information from a first computer to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter; and

transmitting a voted electronic ballot from a second computer to the computer database that resides on the transaction repository server.

24. The method of claim 23, wherein the second computer is the first computer.

25. The method of claim 23, comprising:

transmitting a blank electronic registration form, upon request at the first computer, to the first computer.

26. The method of claim 25, comprising:

transmitting a blank electronic ballot, upon request by the registered voter at the second computer, from the computer database that resides on the transaction repository server to the second computer.

27. The method of claim 23, wherein the step of transmitting registration information comprises:

entering the registration information; and

digitally signing the registration information using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of a citizen, and wherein the

public-private key pair and the cryptographic identification are created prior to transmitting the registration information.

28. The method of claim 27, wherein the public-private key pair and the cryptographic identification can be used by the citizen with respect to a plurality of electronic transactions.

29. The method of claim 26, wherein the step of transmitting a blank electronic ballot comprises:

digitally signing the blank electronic ballot using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of an operator of the transaction repository server, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the blank electronic ballot; and

transmitting a public key of a public-private key pair of the transaction repository server.

30. The method of claim 23, wherein the step of transmitting the voted electronic ballot comprises:

executing the blank electronic ballot;

encrypting the voted electronic ballot using a symmetric cryptographic function and a symmetric key that is randomly generated by the second computer;

encrypting the symmetric key using a public key of a public-private key pair of the transaction repository server; and

digitally signing the encrypted voted electronic ballot and the encrypted symmetric key using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of the registered voter, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the voted electronic ballot.

31. The method of claim 30, comprising:

decrypting the encrypted symmetric key using a private key of the public-private key pair of the transaction repository server;

decrypting the encrypted voted electronic ballot using the symmetric key to recover the voted electronic ballot; and

printing the voted electronic ballot.

32. A method for completing and submitting an electronic registration form and an electronic ballot over a network, comprising the steps of:

transmitting a blank electronic registration form, upon request at a first computer, to the first computer; and

transmitting registration information from the first computer to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter.

33. The method of claim 32, comprising:

transmitting a blank electronic ballot, upon request by the registered voter at a second computer, from the computer database that resides on the transaction repository server to the second computer.

34. The method of claim 33, wherein the second computer is the first computer.

35. The method of claim 33, comprising:

transmitting a voted electronic ballot from the second computer to the computer database that resides on the transaction repository server.

36. The method of claim 32, wherein the step of transmitting registration information comprises:

entering the registration information; and

digitally signing the registration information using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of a citizen, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the registration information.

37. The method of claim 36, wherein the public-private key pair and the cryptographic identification can be used by the citizen with respect to a plurality of electronic transactions.

38. The method of claim 33, the step of transmitting a blank electronic ballot comprises:

digitally signing the blank electronic ballot using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of an operator of the transaction repository server, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the blank electronic ballot; and

transmitting a public key of a public-private key pair of the transaction repository server.

39. The method of claim 35, wherein the step of transmitting the voted electronic ballot comprises:

executing the blank electronic ballot;

encrypting the voted electronic ballot using a symmetric cryptographic function and a symmetric key that is randomly generated by the second computer;

encrypting the symmetric key using a public key of a public-private key pair of the transaction repository server; and

digitally signing the encrypted voted electronic ballot and the encrypted symmetric key using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of the registered voter, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the voted electronic ballot.

40. The method of claim 39, comprising:

decrypting the encrypted symmetric key using a private key of the public-private key pair of the transaction repository server;

decrypting the encrypted voted electronic ballot using the symmetric key to recover the voted electronic ballot; and

printing the voted electronic ballot.

41. A system for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising:

a transaction repository server for transmitting a blank electronic ballot to a first computer;

a computer database, accessible by the transaction repository server, for storing the blank electronic ballot; and

a transaction mediator for communicating information between the transaction repository server and the first computer, the transaction mediator being operative to transmit registration information from the first computer to the computer database to establish a registered voter.

42. The system of claim 41, wherein the transaction mediator is operative to transmit the voted electronic ballot from the first computer to the computer database.

43. The system of claim 42, wherein the first computer comprises multiple computers.

44. The system of claim 41, comprising:

an encrypted communication channel between the first computer and the transaction mediator, and an encrypted communication channel between the transaction mediator and the transaction repository server.

45. The system of claim 41, wherein the registration information includes at least one descriptive element associated with the citizen.

46. A system for verifying at least one of a voter registration status and an electronic ballot status in a voting system, comprising:

a first computer for requesting a status from a transaction repository server; and

at least one computer database, accessible by the transaction repository server, for containing information associated with at least one of the voter registration status of a citizen and the electronic ballot status;

the transaction repository server being operative for determining a status message in response to the status request by examining the at least one computer database, and for transmitting the status message to the first computer.

47. The system of claim 46, wherein the voter registration status of the citizen and the electronic ballot status are verified.